Sheet # 3
Asymmetric-Key Cryptography

Review Questions

1. In asymmetric-key cryptography, how many keys are needed if Alice and Bob want to communicate with each other?
2. In asymmetric-key cryptography, can Alice use the same key to communicate with both Bob and John? Explain your answer
3. In asymmetric-key cryptography, if every person in a group of 10 people needs to communicate with every other person in another group of 10 people, how many secret keys are needed?
4. In asymmetric-key cryptography, if e very person in a group of 10 people needs to communicate with every other person in the group, how many secret keys are needed?

Exercises

1. In RSA, given two prime numbers p=19 and q=23, find n and φ. Choose e=5 and try to find d, such that e and d meet the criteria. If plaintext =3, what will be the cipher text?
2. Use RSA algorithm to encrypt and decrypt the word "BE" using the key pairs (3, 15) and (5, 15).
3. To understand the security of the RSA algorithm, find d if you know that e=17 and n=187. This exercise proves how easy is for Eve to break the secret if n is small.
4. For the RSA algorithm with a large n, explain why Bob can calculate d from n, but Eve cannot.
5. Using e=13, d=37, and n=77 in the RSA algorithm, encrypt the message "FINE" using the values of 00 to 25 for letters A to Z. For simplicity, do the encryption and decryption character by character.
6. Why can't Bob choose 1 as the public key e in RSA?
7. ***(Report)*** What is the danger in choosing 2 as the public key e in RSA?
8. Alice uses RSA to send a message to Bob, using Bob's public key. Later, at a cocktail party, Eve sees Bob and asks him if the message has arrived and Bob confirms it. After a few drinks, Eve asks Bob, "What was the ciphertext?" Bob gives the value of the ciphertext to Eve. Can this endanger the security of Bob's private key? Explain your answer.
9. What is the value of the symmetric key in the Diffie-Hellman protocol if g=7, p=23, x=2, and y=5?
10. In the Diffie-Hellman protocol, what happens if x and y have the same value? That is, Alice and Bob have accidentally chosen the same number. Are the values of R_1 and R_2 are the same? Are the values of the session keys calculated by Alice and Bob the same? Use an example to prove your claims.